PX145

From: [redacted]
To:
Sent: 1/16/2018 10:24:27 AM
Subject: Charlie Noyes blog post on Telegram ICO

Charles Noyes<https://tokeneconomy.co/@csnoyes?source=post_header_lockup>Follow
Blockchain analyst and quantitative trader at Pantera Capital. MIT EECS.
Jan 13
$600 Million TONs of Crap

Telegram is a nice messenger app but it is neither as secure nor as trusted as Signal, which I use for any communication that requires actual privacy, for a very simple reason. See the below quote by an actual expert:
"They use the MTproto protocol which is effectively homegrown and I've seen no proper proofs of its security," Alan Woodward, professor at the University of Surrey. Woodward criticized Telegram for their lack of transparency regarding their home cooked encryption protocol. "At present we don't know enough to know if it's secure or insecure. That's the trouble with security by obscurity. It's usual for cryptographers to reveal the algorithms completely, but here we are in the dark. Unless you have considerable experience, you shouldn't write your own crypto. No one really understands why they did that."

This is the Telegram approach to doing things. It is incompatible with blockchain technology; the Bitcoin whitepaper gives a clear enough specification of how it will work that any well enough informed researcher could validate the core ideas. The stuff that does go unsaid has introduced massive headaches; the blocksize is one such example, the necessity of SegWit or FlexTrans, etc. All of those issues cropped up from pure implementation details.

You cannot mess up something decentralized in a fundamental way; anything less than absolute correctness is absolute failure. Even though Bitcoin is fundamentally perfect (with regard to its ability to not die in a fire), there are enough implementation issues that everyone is still arguing about how best to fix them, and whether hard forking to fix them will destroy the ability for anyone to trust it. Even though I believe hard forks are needed in our improvement toolbox, using them as a crutch for potentially completely broken, homegrown things is not good. And I imagine Telegram will have to use them that way in their blockchain, as soon as the first couple hundred dumb, avoidable issues crop up. Without outside scrutiny this is to be expected.

Telegram/TON's 132 page whitepaper says nothing substantial about the hard parts of designing a decentralized protocol. It is essentially a wishlist of things they want to have, and how it will work assuming that their wishlist doesn't crash and burn. It does not make any substantial contributions to proof of stake research. It does not make any substantial contributions to sharding research. It does not make any substantial contributions to "hypercube routing" research. Articles like the one TechCrunch put out on this<https://techcrunch.com/2018/01/08/telegram-open-network/>are laughable. The entire thing should have a disclaimer attached:"all of the technical things we said this will do are completely unproven and have not been subjected to outside scrutiny."

Their infinite sharding and "hypercube routing" plans flow from earlier, now abandoned, proposals by Vitalik Buterin (e.g. hypercube routing is literally a blog post of his<https://blog.ethereum.org/2014/10/21/scalability-part-2-hypercubes/>, now memorialized in the graveyard of Ethereum's prehistory<http://vitalik.ca/general/2017/09/14/prehistory.html>). The whitepaper does not say anything about why they will be able to do things Vitalik cannot (such as have 2^{9} self-rebalancing shards), and it is insane to say it's because he can't hard fork Ethereum[1]. He already has, many times, and there are many more hard forks planned to change fundamental properties of the Ethereum network[2]. But all of those changes are discussed, debated, and, if disproven, abandoned. In 132 pages they've managed to summarize the state of current blockchain research and make no provable claims about its future.

The last point is why we don't like TON. I do not know how it will work. I cannot, in 132 pages, gain the slightest intuition as to how to go about proving that the hard problems it needs to solve will be solved. It's not just that it isn't a bulletproof specification; I don't even know how to begin evaluating if it will work at all, and I'm speaking as at least a moderately informed protocol analyst. I might throw house money into this with no

lockup and at a lower valuation. I probably wouldn't even throw house money into this under the actual lockup and valuation, but I still might. I certainly would not put a single cent I care more than nil about losing into this.

Mostly, because I think that this is an opportunistic ploy. Holding a sale while disallowing the release of the technical whitepaper restricts the class of people able to evaluate it to those that are both technically able to and also able to invest. That is almost the null set. It is antithetical to the entire philosophy of the space, and the actual terms of the raise are similar to selling a massively out of the money call option on a biotech that promises a drug to cure cancer without allowing anyone but investors to see the underlying research, 99.999[1] of whom are not equipped to evaluate it. It's peer review by venture capitalist.

---

1 This claim was made by the TON team during a fundraising meeting.
2 Vitalik is used, I think fairly, to symbolize the wishes of the Ethereum development community.

Edit/A note: the MTproto example is just to illustrate that this has always been their operating model: security by obscurity. MTproto is an orthogonal problem to that of their TON tech, both stemming from either their inability or distaste to subject themselves to rigorous external scrutiny. Security by obscurity may be palatable for a messaging app (at least if you don't live in an authoritarian state); it is death for a blockchain.